RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: LAW-W01

Battlefield Hackers and the Rules They Must Follow

Laura Walker McDonald

Senior Advisor on New Technologies & Conflict
International Committee of the Red Cross

Jonathan Horowitz

Deputy Head, Legal Department – Washington, D.C.
International Committee of the Red Cross

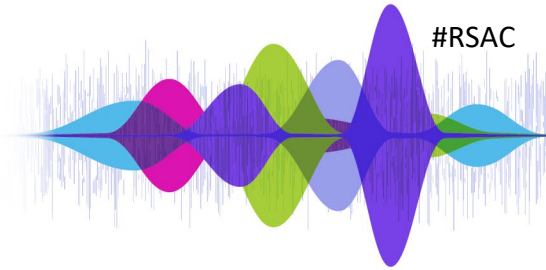
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Evolution of the Cyber Environment in Situations of War



- Cyber operations at the frontline combined with electromagnetic activities (CEMA) to establish extended A2AD (Anti-Access/Area Denial) areas.
- Response with ADA2 platforms (All-Domain Attritable Autonomous Systems). Autonomy in offensive operations.
- Increasing cyber operations against OT (Operational Technology), ICS (Industrial Control System), SCADA (Supervisory Control and Data Acquisition) systems of indispensable objects to the survival of civilian populations.

Patterns and Trend in the Tactics, Techniques, and Effects of Civilian Hackers

- Increased sophistication in DDoS operations (L7 and L3/L4 layers – Rapid Reset, Continuation Flood, etc.).
- Disruptive and destructive operations against ISP, in coordination with EW: reverberating effects.
- Disruptive and destructive operations against OT: from low hanging fruits to exploitation of known vulnerabilities.
- Development and deployment of ransomware by civilian hacker collectives. RaaS from the criminal market.

RSAC 2025 Conference

Wartime Prohibitions on Cyber Operations

Wartime Prohibitions on Cyber Operations

- The “law of armed conflict” / ”international humanitarian law” place limits on how wars may be fought. (See, generally, the rules set forth in Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land,1907; the Four Geneva Conventions, including Common Art 3; Additional Protocols I & II; and Customary International Humanitarian Law. More specifically, see Additional Protocol I’s “basic rule” Art 35 (“In any armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited.”)
- The purpose of these rules is to protect civilians and others from the harms of conflict. (Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, 1907, Preamble (“Thinking it important, with this object, to revise the general laws and customs of war, either with a view to defining them with greater precision or to confining them within such limits as would mitigate their severity as far as possible”); for the Fourth Geneva Conventions, see Mačák K, Policinski E. IN PURSUIT OF A TREATY'S SOUL: A STUDY OF THE OBJECT AND PURPOSE OF THE FOURTH GENEVA CONVENTION. *International and Comparative Law Quarterly*. 2024;73(2):385-415; Additional Protocol I, Preamble (“‘Believing’ it necessary nevertheless to reaffirm and develop the provisions protecting the victims of armed conflicts and to supplement measures intended to reinforce their application”), Additional Protocol II, Preamble (“‘Emphasizing’ the need to ensure a better protection for the victims of those armed conflicts”))
- Warring parties must follow these rules. (Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, 1907, Art 1; Four Geneva Conventions, Common Art 1 (“The High Contracting Parties undertake to respect and to ensure respect for the present Convention in all circumstances”); Additional Protocol I, Art 1 (“The High Contracting Parties undertake to respect and to ensure respect for this Protocol in all circumstances.”) & Additional Protocol II, Art 1 (“each Party to the conflict shall be bound to apply, as a minimum, the following provisions:…”)
- The laws of war apply to cyber actors. (Numerous States; and Res. on ICTs from the 34th International Conference of the Red Cross and Red Crescent, para. 4 (“reiterates that, in situations of armed conflict, IHL rules and principles – including the principle of distinction, the prohibition of indiscriminate and disproportionate attacks, the obligations to spare the civilian population, civilians and civilian objects in the conduct of military operations, and to take all feasible precautions to avoid, and in any event minimize, incidental civilian harm, the prohibition of encouraging or inciting violations of IHL, and the prohibition of acts or threats of violence, the primary purpose of which is to spread terror among the civilian population – serve to protect civilian populations and other protected persons and objects, *including against the risks arising from ICT activities*” Emphasis added.)
- Hackers must follow these rules. (Four Geneva Conventions, Common Art 1 & Nuremburg Trials, see ICRC Commentary to Common Article 1, paras 183-189).

DoD Law of War Manual (2023)

- "The law of war affirmatively anticipates technological innovation and contemplates that its existing rules will apply to such innovation, including cyber operations" §16.2.1
  - (e.g., "If a cyber operation constitutes an attack, then the law of war rules on conducting attacks must be applied to those cyber operations" §16.5.1)
- "Precisely how the law of war applies to cyber operations is not well settled, and aspects of the law in this area are likely to continue to develop, especially as new cyber capabilities are developed and States determine their views in response to such developments." §16.1

Eight Wartime Rules Civilian Hackers Must Follow

Do not direct cyber attacks against civilian objects. (Additional Protocol I, Art 48 & Art 52; Customary International Humanitarian Law, Rule 7; numerous States; Res. on ICTs from the 34th International Conference of the Red Cross and Red Crescent, para. 4)

Do not use malware or other tools or techniques that spread automatically and damage military objectives and civilian objects indiscriminately. (Additional Protocol I, Art. 51(4); Customary International Humanitarian Law, Rule 11; numerous States; Res. on ICTs from the 34th International Conference of the Red Cross and Red Crescent, para. 4)

When planning a cyber attack against a military objective, do everything feasible to avoid or minimize the effects your operation may have on civilians. (Additional Protocol I, Art. 57; Customary International Humanitarian Law, Rule 15; numerous States; Res. on ICTs from the 34th International Conference of the Red Cross and Red Crescent, para. 4)

Do not conduct any cyber operation against medical and humanitarian facilities. (First, Second, and Fourth Geneva Conventions; Additional Protocol I, Part II, Sections 1-2, Art 70(4) & Additional Protocol II, Art 9, Art 10, Art 11, Art. 18(2), Customary International Humanitarian Law, Rule 25, Rule 26, Rule 28, Rule 29, Rule 31, & Rule 32, States positions here & here, Res. on ICTs from the 34th International Conference of the Red Cross and Red Crescent, para. 6)

Eight Wartime Rules Civilian Hackers Must Follow

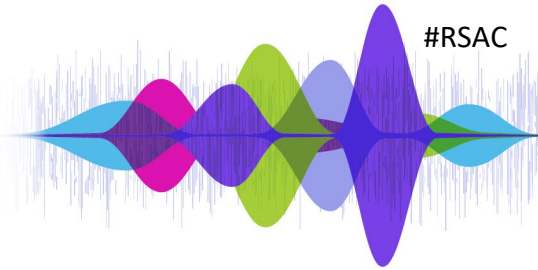
Do not conduct any cyber attack against objects indispensable to the survival of the population or that can release dangerous forces. (Additional Protocol I, Art 54 & Additional Protocol II, Art 14; Customary International Humanitarian Law, Rule 54; State positions)

Do not make threats of violence to spread terror among the civilian population. (Additional Protocol I, Art 51(2) & Additional Protocol II, Art 13(2); Customary International Humanitarian Law, Rule 2; Res. on ICTs from the 34th International Conference of the Red Cross and Red Crescent, para. 4)

Do not incite violations of international humanitarian law. (Four Geneva Conventions, Common Art 1; Additional Protocol I, Art 1; Res. on ICTs from the 34th International Conference of the Red Cross and Red Crescent, para. 4)

Comply with these rules even if the enemy does not. (Four Geneva Conventions, Common Art 1; Additional Protocol I, Art 1; Customary International Humanitarian Law, Rule 140; International Court of Justice and Nuremberg Trails, see sources in commentary to Rule 140)

Applying this Knowledge



- Limit civilian exposure to the digital crossfire of war.
  - Map out the foreseeable direct and indirect effects of cyber operations on civilians and essential civilian services.
  - Know and abide by the rules of IHL/LOAC, incl. by not directing operations against civilians, and avoiding, or at least minimizing, incidental civilian harm.
- Build communities and share tools, tactics, and techniques that protect civilians from the harms of cyber operations.

RSAC 2025 Conference

Many Voices.
One Community.

Thank You

Contact us on LinkedIn or:

Laura Walker McDonald: lwalkermcdonald@icrc.org

Jonathan Horowitz: jhorowitz@icrc.org